A METHOD OF LIMITING THE AMOUNT OF NETWORK TRAFFIC REACHING A LOCAL NODE OPERATING ACCORDING TO AN INDUSTRIAL ETHERNET PROTOCOL

PROCÉDÉ DE LIMITATION DE LA QUANTITÉ DÉ TRAFIC ATTEINDRE D’UN NOEUD OPÉRANT SELON UN PROTOCOLE ETHERNET INDUSTRIEL

Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

Date of publication of application:
09.05.2012 Bulletin 2012/19

Propietor: ABB Research Ltd.
8050 Zürich (CH)

Inventors:
• MCGRATH, Kevin
  N-0254 Oslo (NO)
• WOLD, Alexander
  N-1412 Sofiemyr (NO)

Representative: Ahrengart, Kenneth
ABB AB
Intellectual Property
Ingenjör Bååths Gata 11
721 83 Västerås (SE)

References cited:

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).
Description

TECHNICAL FIELD.

[0001] The present invention is concerned with an electronic device used in an industrial context. In particular it is concerned with an electronic device used in or connected to a system for monitoring and control such as a system for generation, transmission or distribution of electricity or for an industrial process control system.

TECHNICAL BACKGROUND

[0002] Many electronic devices in modern control systems are arranged with some kind of built-in intelligence. Such devices are often a part of or referred to as embedded devices. Control systems for industrial process control and systems for control in generation, distribution and transmission of electricity are often connected to the industrial equipment the control system monitors and controls via one or more data communication networks that use open protocols such as Ethernet based protocols. This has standardised and simplified industrial data communication for the purposes of monitoring and control. Electronic devices that may be connected to a control system using an industrial Ethernet standard are included in many and various devices, for example instruments such as sensors or transducers, actuators such as valves, motors, pumps, switches, as well as controls on major equipment such as generators, transformers, breakers, power trains and so on.

[0003] Due to limited processing resources, resource constrained electronic devices or embedded devices can easily be overwhelmed by deliberate (or accidental) excessive network traffic. Under such conditions packet filtering is needed in order to limit the amount of traffic. Legitimate traffic needs to pass while at the same time unwanted traffic has to be discarded. Because of the limited processing resources of a resource constrained electronic device, it is challenging to implement this functionality as a software solution in a small electronic device with limited computing resources.

[0004] Network traffic filtering is generally done with software filtering, or an external firewall, or a combination of those. External firewalls require additional engineering, and may rely on products manufactured by third parties. In such firewalls or software filters, the filtering of unwanted traffic has to be discarded. Because of the limited processing resources of a resource constrained electronic device, it is challenging to implement this functionality as a software solution in a small electronic device with limited computing resources.

[0005] US6,434,118 entitled Method for determining round trip time utilizing ATM traffic management mechanism, assigned to 3COM Corporation, mentions in the context of testing to establish a round trip time that a CRC error can be purposely placed in a Ethernet frame which causes the MAC layer in the destination to drop the frame and prevent it from reaching the upper layers. US7,280,591 entitled Integrated reduced media independent interface, assigned to Via technologies, describes an integrated reduced media independent interface (Integrated RMII) and related method for interconnecting a MAC Circuit and a PHY Circuit.

[0006] US2004/073671 discloses a method and apparatus for filtering data packets including a packet filter processor arranged between a physical layer and a data link layer in a network stack. The packet filter processor is designed such that the processor is directed to look at the source IP address of each received data packet to determine if the source IP address matches one of a plurality of stored source IP addresses, and if there is a match, then discard or forward the data packet depending on the data configuration.

SUMMARY OF THE INVENTION

[0007] The aim of the present invention is to remedy one or more of the above mentioned problems. This and other aims are obtained by a method characterised by claim 1.

[0008] According to a first aspect of the invention a method is disclosed to limit the amount of network traffic reaching a local node in an electronic device operating an Ethernet networking protocol and using a network stack comprising at least one physical layer communicating with at least one link layer where the data received is propagated to one or more higher layers of said network stack, said electronic device being connected to a communication network, in which method said network traffic is filtered and an unwanted data reception addressed to said electronic device filtered out, said method comprising receiving said network traffic in at least one said physical layer of said electronic device, detecting a said unwanted data reception, and discarding the said unwanted data reception in a link layer device or media access controller (MAC) before it reaches another higher layer of said network stack of said electronic device.

[0009] According to another embodiment of the invention, a method is disclosed to limit the amount of network traffic reaching a local node in an electronic device operating an Ethernet networking protocol and using a network stack comprising at least one physical layer communicating with to at least one link layer where the data received is propagated to one or more higher layers of said network stack, said electronic device being connected to a communication network, in which method said network traffic is filtered and an unwanted data reception addressed to said electronic device filtered out, said method comprising receiving said network traffic in at least one said physical layer of said electronic device, detecting a said unwanted data reception, and discarding the said unwanted data reception in a link layer device or media access controller (MAC) before it reaches another higher layer of said network stack of said electronic device.

[0010] According to another embodiment of the invention, a method is disclosed to limit the amount of network traffic reaching a local node in an electronic device operating an Ethernet networking protocol and using a network stack comprising at least one physical layer com-
According to another embodiment of the invention, a method is disclosed to limit the amount of network traffic reaching a local node in an electronic device operating an Ethernet networking protocol and using a network stack comprising at least one physical layer communicating with at least one link layer where the data received is propagated to one or more higher layers of said network stack, said electronic device being connected to a communication network, in which method said network traffic is filtered and an unwanted data reception addressed to said electronic device filtered out, said method comprising detecting said unwanted data reception and asserting a control signal in a media access controller of the said electronic device by switching a line, bus or circuit to a predetermined potential such that a media access controller (MAC) of the link layer rejects the said unwanted data reception transmitted from the physical layer.

According to another embodiment of the invention, a method is disclosed to limit the amount of network traffic reaching a local node in an electronic device operating an Ethernet networking protocol and using a network stack comprising at least one physical layer communicating with at least one link layer or media access controller (MAC). An advantage of this embodiment is that filtering may be activated when a need is perceived or is not activated unnecessarily. This information may also be combined with other data reception information to determine when filtering may be switched on or off.

According to another embodiment of the invention, a method is disclosed to limit the amount of network traffic reaching a local node in an electronic device operating an Ethernet networking protocol and using a network stack comprising at least one physical layer communicating with at least one link layer where the data received is propagated to one or more higher layers of said network stack, said electronic device being connected to a communication network, in which method said network traffic is filtered and an unwanted data reception addressed to said electronic device filtered out, said method comprising inspecting said network traffic during reception from the at least one said physical layer (PHY) to at least one said link layer or media access controller (MAC); or by switching on filtering dependent on the number of data packets received per unit time according to at least one predetermined number of data packets.
According to another embodiment of the invention, a method is disclosed to limit the amount of network traffic reaching a local node in an electronic device operating an Ethernet networking protocol and using a network stack comprising at least one physical layer communicating with at least one link layer where the data received is propagated to one or more higher layers of said network stack, said electronic device being connected to a communication network, in which method said network traffic is filtered and an unwanted data reception addressed to said electronic device filtered out, said method comprising inspecting said network traffic during reception from the at least one said physical layer (PHY) to at least one said link layer or media access controller by comparing with data in any from the group of: a list of accepted traffic, information based on an analysis of traffic, a list updated by a processor of said electronic device, a list of non-accepted traffic, an access control list.

In the first aspect of the invention a method is provided which limits the effects of some network denial of service attacks on an embedded networked device. The method increases the responsiveness of resource-constrained systems suffering from an accidental or deliberate excess of network traffic such as during a denial of service (DOS) attack. The method limits the amount of data received by the network stack of an electronic device such as an embedded device, thereby reducing central processing unit (CPU) utilization. The term CPU is used to describe both microprocessors and microcontrollers. Based on certain parameters, only selected traffic is allowed to propagate through the network stack of the electronic device, with zero or constant near zero latency being added by this filtering process. By inspecting traffic during reception and rejecting a transmission detected to be unwanted, the unwanted traffic is stopped before it reaches the CPU. This way, legitimate traffic can pass with zero or constant near zero latency. The term "during reception" refers to a packet which is in the process of being received by the electronic device.

An important advantage of the described method and circuit is that network traffic is filtered without affecting latency because the filtering of packets takes place during propagation, meaning during reception in the electronic device. There is no pre-filtering. The data packets are filtered while they are being received by the electronic device.

Another advantage is that this invention may be implemented in an embedded system in a simple way. Preferably a hardware circuit such as a field programmable gate array (FPGA) or application-specific integrated circuit (ASIC) is connected between two circuits of the electronic device.

The invention could also be integrated directly in the PHY circuit or the media access controller (MAC) circuit, or integrated in a CPU. CPUs targeting networked embedded systems often contain a MAC and the invention could then be integrated with such a CPU, or another CPU which has an integrated MAC and also further a CPU that has a MAC and a PHY integrated.

The invention can also be extended with further ways to detect unwanted traffic, however this description does not elaborate on ways of detecting unwanted traffic, but rather describes how detected unwanted traffic is stopped with minimal latency.

One technical result of this invention implemented in an electronic device is increased network robustness at a low cost. Another advantage when compared to an external firewall, is that the invention also does not require user configuration, or additional engineering tools. Further, a deterministic constant latency firewall, may have use cases in low latency real-time Ethernet applications. In electronic devices or systems which already employ a circuit such as a field programmable gate array (FPGA), using the methods, teachings and so on of an embodiment of the invention it is likely that these features will add little or no additional costs to the existing production cost of the electronic device.

As noted above, an advantage of the described method is the zero or constant near zero latency introduced when filtering. A frame, Ethernet frame, packet and data packets and variations of the terms have a similar meaning in this description. Known firewalls typically read the whole Ethernet frame before making a decision on how to handle the packet. The Ethernet frame is then either transmitted or discarded. Reading the complete frame introduces additional latency, which latency is also variable dependent on the frame length, and may be considerable depending on the structure or content of one or more of the data packets.

In contrast, the described method filters network traffic with a zero or Constant near zero latency. The filtering happens after reception has started in the physical layer, while the received frame is propagated to the Ethernet MAC. The detection part of the filtering may be started on data forming a partially received data packet. The detection may also or instead be carried out only after a complete data packet has been received. In any case, if an unwanted frame is detected, the RX_ERROR bus line or other control signal of the media independent interface bus (MII), or similar bus is asserted. When the Ethernet MAC detects this control signal the frame is dropped as though it contained an error. Alternatively on a high speed serial bus not having separate control and data signals, control data can be appended to the frame in order achieve the same result.

According to another aspect of the invention, an electronic device is disclosed comprising a local node arranged for operation according to an Ethernet networking protocol using a network stack comprising at least
one physical layer (PHY) and communication to at least one link layer or media access controller, said electronic device having a serial interface for connection to a communication network, wherein said network traffic to said electronic device may be filtered and an unwanted data reception addressed to said electronic device filtered out, which electronic device also comprises a filtering unit connected between said at least one physical layer (PHY) and the link layer or media access controller (MAC), the filtering unit being arranged with at least one switchable line or bus and control logic for inspecting said network traffic during reception from the at least one said physical layer to at least one said link layer or media access controller, and for comparing said network traffic to at least one access control list and for detecting a said unwanted data reception, the filtering unit being arranged for sending a signal causing the selected said unwanted data reception to be rejected and discarded by the at least one said link layer or media access controller before it reaches another layer of said network stack.

According to another embodiment of the invention, an electronic device is disclosed comprising a local node arranged for operation according to an Ethernet networking protocol using a network stack comprising at least one physical layer (PHY) and communication to at least one link layer or media access controller, said electronic device having a serial interface for connection to a communication network, wherein said network traffic to said electronic device may be filtered and an unwanted data reception addressed to said electronic device filtered out, wherein the electronic device also comprises that the filtering unit is arranged for asserting a control line error by means of the switchable line or bus, upon detection of a said unwanted data reception.

According to another embodiment of the invention, an electronic device is disclosed comprising a local node arranged for operation according to an Ethernet networking protocol using a network stack comprising at least one physical layer (PHY) and communication to at least one link layer or media access controller, said electronic device having a serial interface for connection to a communication network, wherein said network traffic to said electronic device may be filtered and an unwanted data reception addressed to said electronic device filtered out, wherein the filtering unit of the electronic device is arranged for appending control data upon detection of a said unwanted data reception.

According to another embodiment of the invention, an electronic device is disclosed comprising a local node arranged for operation according to an Ethernet networking protocol using a network stack comprising at least one physical layer (PHY) and communication to at least one link layer or media access controller, said electronic device having a serial interface for connection to a communication network, wherein said network traffic to said electronic device may be filtered and an unwanted data reception addressed to said electronic device filtered out, wherein the electronic device comprises apparatus or control logic for determining a number of data packets received per unit time.

According to another embodiment of the invention, an electronic device is disclosed comprising a local node arranged for operation according to an Ethernet networking protocol using a network stack comprising at least one physical layer (PHY) and communication to at least one link layer or media access controller, said electronic device having a serial interface for connection to a communication network, wherein said network traffic to said electronic device may be filtered and an unwanted data reception addressed to said electronic device filtered out, wherein the electronic device is connected to an external circuit from which it can receive information for determining in the control logic a number of data packets received per unit time.

According to another embodiment of the invention, an electronic device is disclosed comprising a local node arranged for operation according to an Ethernet networking protocol using a network stack comprising at least one physical layer (PHY) and communication to at least one link layer or media access controller, said electronic device having a serial interface for connection to a communication network, wherein said network traffic to said electronic device may be filtered and an unwanted data reception addressed to said electronic device filtered out, wherein the electronic device comprises apparatus for logging data (47) concerning discarded unwanted data packets and/or recording characteristics about the network traffic.

A computer program, and a computer program recorded on a computer-readable medium is disclosed in another aspect of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the method and system of the present invention may be had by reference to the following detailed description when taken in conjunction with the accompanying drawings wherein:

Figure 1 shows a schematic block diagram from a known Ethernet networking protocol or standard;
Figure 2 shows a schematic block diagram of a circuit or device connected between a PHY and a MAC unit according to an embodiment of the invention;
In a first aspect of the invention a method is

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0033] In a first aspect of the invention a method is implemented which blocks selected network traffic by relying on features present in the Ethernet MAC. The MAC by design, does not propagate packets which are malformed or packets when the MII reception error bus line RX_ERROR is asserted. On other busses where the control signals do not have dedicated separate bus lines, the MAC by design does not propagate packets that are marked with control data indicating an error. (A MAC circuit will also discard a data packet that is valid but has the wrong MAC address, an incorrect MAC address.) A preferred implementation of the invention is a circuit connected between the Ethernet PHY and the Ethernet MAC. Ethernet frames sent by the Ethernet PHY and dropped by the Ethernet MAC do not impact CPU performance. The invention can be implemented with a simple electronic device such as a field programmable gate array, FPGA requiring only a limited amount of resources. Alternatively the invention could be integrated in a PHY, MAC, CPU or other circuit.

[0034] Figure 1 shows a part of a known, standard Ethernet networking protocol illustrating the connection of a physical layer circuit (PHY) 1 to a media access controller (MAC) 2. The PHY and the MAC is the interface between the physical layer and the link layer. The terms link layer and data link layer are used interchangeably.

[0035] Figure 3 shows a general use of a widely known model, the OSI Open Systems Interconnection Reference Model. This model describes seven conceptual layers:

31. Physical layer 1,
32. Data link layer 2,
33. Network layer 3,
34. Transport layer 4,
35. Session layer 5,
36. Presentation layer 6 and
37. Application layer 7.

[0036] A layer in the OSI model is a collection of conceptually similar functions that provide services to the layer above it and receives service from the layer below it. (See ISO/IEC TR 8802-1:2001 or any standard text about IEEE 802 standards for more information about the OSI model and the variations applicable to different networking standards.) Within some standards, for example IEEE 802 LAN architectures, the Link Layer 2 comprises or is arranged with a Media Access Control (MAC) circuit. The MAC typically provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multipoint network, such as a local area network (LAN).

[0037] Figure 2 shows a circuit 3 connected between the PHY and the link layer comprising a MAC unit or circuit. The Figure shows a filtering unit in the form of a filtering circuit 3 compatible with the MII bus connected between the PHY and MAC unit. The circuit 3 may be embodied in the form of a media independent interface or MII. The MII bus between the PHY 1 and the MAC 2 is arranged with a separate data line RX-D 11 and control line RX_ERROR 12. The figure shows that the filtering circuit has a temporary memory or registers 4, filter memory 6, an interface to an external circuit 20, for instance a CPU. The filtering circuit or unit also has a control unit or control logic 8. An error detecting interface in the MII, preferably a reception error bus or line RX_ERROR 9, is connected to a signal line to the MAC 2. The media independent interface (MII) may be a reduced media independent interface (RMII) or another variation of a media independent interface, such as a Gigabit media independent interface (GMII), reduced Gigabit media independent interface (RGMI) or other bus with separate control and data lines.

[0038] In Figure 2 the PHY 1 is connected directly to the MAC 2, and the circuit 3 is also connected to the same bus. RX_ERROR is connected through the circuit 3 between PHY and MAC. The circuit has a list of traffic rules, or an access control list, preferably stored in filter memory storage device 6, used for comparison to detect unwanted or wanted network traffic, and this list may be

(a) constructed based on traffic analysis or,
(b) a list updated by the embedded system of the electronic device or,
(c) a list of unwanted traffic (blacklist) or,
(d) a list of legitimate traffic (whitelist),
(e) a list provided by the vendor,
(f) a list based on the environment which the embedded system is operating in,
(g) a list from another source,
The traffic rules may be updated and changed by the system, for instance by information routed through external circuit 20 or in the control logic 8. The filtering may be turned on or off, thus letting traffic which matches the list pass without asserting the bus control line when off. When turned on the filtering asserts the bus control line RX_ERROR or another control line, when unwanted data is detected. The selection criteria for turning the filtering scheme on or off may comprise criteria such as:

(a) a limit on number of packets per time unit. The number of packets per time unit may be supplied by the embedded system, or
(b) selectively by the CPU, or
(c) by other means.

Significantly, the filtering circuit 3 does not delay Ethernet Frames by storing them and sending them to the MAC at a later time. The rejected Ethernet frames are discarded, rejected by the MAC circuit in the link layer, and do not reach other layers (such as layers conforming with the OSI model layers 33-37 see Fig 3,) in the network stack of the processor in the embedded network device.

When active, the decision logic module circuit or control logic 8 checks the content of the Ethernet Frames, and matches this to the access control list containing the traffic rules. If there is, for example no match with any data in a white list, the circuit 3 asserts RX_ERROR line 9 of the media independent interface (MII) or other control (RX_ERROR 12) to indicate an error in the Ethernet Frame (see Figure 2).

The number of data packets received per unit time is noted and may be recorded. This may be carried out within the control logic 8 of the filtering unit 3, or it may be carried out by receiving through a line in to the filtering unit, for example from external circuit 20, information from an external device or circuit about the rate of packets received, which information may be calculated or processed in the control logic 8 to arrive at a rate of data packets received per unit time. Filtering may optionally be switched on when the number of data packets received per unit time reaches or exceeds a predetermined number. The number of discard events when unwanted data packets are discarded may be detected and preferably recorded. Data concerning discarded unwanted data packets may be logged and/or information recorded about characteristics such as the amount of network traffic, time of data packet discard. Discarded traffic may be logged by the filtering circuit and stored for processing at a later time. See also step 47 of Fig 4 and described below in relation to Figure 4.

A practical and implementable way to filter incoming data transmissions is to compare them with a list of accepted traffic. A white list of network traffic is intended to facilitate normal communication with a device suffering some denial of service attacks. The following invariants are defined:

1. An upper limit of packets processed per time unit. When this limit is reached, white listed traffic may be discarded.
2. A limit of packets processed per time unit. When this limit is reached, traffic not matched in the white list may be discarded.

The following may be a part of the white listed traffic:

1. A list of open, established connections in the network stack, shall be white listed. This is usually a small amount of information that can be transferred from a CPU of the electronic device which includes the circuit 3 employing the invention.
2. A second list of systems that the electronic device has communicated successfully with in the past.

A blacklist of not acceptable network traffic may also be constructed, and be used instead of, or as well as, the white list.

In another embodiment a bus with similar functionality as the media independent interface (MII) or a bus with similar functionality as the serial Gigabit media independent interface (SGMII) may be arranged embodied together with a PHY and MAC inside a circuit, or combined together with another function in another electronic component. For example included in a chip or circuit including both a MAC function and a PHY function; or a chip or circuit that includes both a processor with other functionality that includes either the MAC or the PHY or both the MAC and the PHY.

In another embodiment such Gigabit Ethernet using a high speed serial bus such as serial gigabit media independent interface (SGMII), a circuit such as shown in Figure 5 may be used. For example Gigabit Ethernet with high speed serial lines where the control lines 11, 12 are missing. For a detected unwanted data packet sending control information after the data, not changing the data, and indicating an error, would result in the same as asserting the MII control lines. The same result can be achieved, that of rejecting a data packet in the MAC after it has been determined to be unwanted during reception in the physical layer, that same result can be achieved by appending control information to the data.

Here the signals are routed thorough the filtering circuit and a Error_Propagation ordered_set or other symbol or control information is added to the reception, thereby notifying the MAC with control information of the decision to discard the data. The data itself is left unchanged and valid. Another method which involves using...
the data line 11 is to change the destination MAC-address of the packet and recalculate the CRC on the fly, thereby producing a valid packet, but with the wrong MAC address, which the MAC discards.

[0049] In yet another embodiment of the invention the circuit connected between the PHY and the MAC which filters packets as they are propagating could be implemented solely in the MAC. This may require that a custom MAC would be needed, however filtering functionality according to the invention could be a feature built into a MAC.

[0050] In yet another embodiment of the invention the circuit connected between the PHY and the MAC which filters packets as they are propagating could be implemented solely in the PHY. This may require that a custom PHY would be needed, however filtering functionality according to an aspect of the invention could be a feature built into a PHY circuit.

[0051] Figure 4 shows a simplified flowchart for one or more methods according to another aspect of the invention. The figure shows:

1. Data for a frame, e.g. Ethernet frame, is received in the physical layer.
2. Data in part or whole of the frame is compared with the traffic rules for filtering;
3. If unwanted data is detected Y - then
4. Control signal asserted or control data appended (so that frame is subsequently discarded in the MAC)
5. If control signal is asserted or control data appended then data about that discarded frame may be logged;
6. If unwanted traffic not detected N then
7. The packet is propagated with original control signal(s) and original data to another network layer 33-37.

[0052] The electronic device may be installed and configured for use in a local node of a component connected to, and controlled by, a control system. Typically as a component controlled by a control system, a component such as a measuring instrument for example a sensor or transducer, or an actuator such as a valve, motor, pump, switch, or another component used in the control of industrial processes such as a pulp & paper process, metal forming process, or for controlling equipment such as transformers, breakers, isolators, switches and so on used eg in feeder installations, switch yards and substations for the generation, transmission or distribution of electrical power.

[0053] The functions of the filtering unit 3 or filtering circuit may be carried out by processing digital functions, algorithms and/or computer programs and/or by analogue components or analogue circuits or by a combination of both digital and analogue functions.

[0054] The methods of the invention may be carried out by means of one or more computer programs comprising computer program code or software portions running on a computer or a processor. The microprocessor (or processors) comprises a central processing unit CPU performing the steps of the method according to one or more facets of the invention. This is performed with the aid of one or more said computer programs, such as, which are stored at least in part in a memory storage device such as memory 6 and/or in control logic 8 and as such accessible by the one or more processors. The or each processor may be in a control unit, or part thereof.

It is to be understood that said computer programs may also be run on one or more general purpose industrial microprocessors or computers instead of one or more specially adapted computers or processors.

[0055] The computer program comprises computer program code elements or software code portions that make the computer perform methods such as that shown in the flowchart of Figure 4 using equations, algorithms, data, stored values and calculations previously described. A part of the program may be stored in a processor as above, but also in a ROM, RAM, PROM, EPROM or EEPROM chip or similar memory means. The program in part or in whole may also be stored on, or in, other suitable computer readable medium such as a magnetic disk, CD-ROM or DVD disk, hard disk, magnetic or optical memory storage means, in volatile memory, in flash memory, as firmware, stored on a data server or on one or more arrays of data servers. Other known and suitable media, including removable memory media such as memory sticks or other removable flash memories, hard drives etc. may also be used.

[0056] It should be noted that while the above describes exemplifying embodiments of the invention, there are several variations and modifications which may be made to the disclosed solution without departing from the scope of the present invention as defined in the appended claims.

Claims

1. A method of limiting the amount of network traffic reaching an electronic device operating an Ethernet networking protocol and using a network stack comprising at least one physical layer (31) communicating with at least one link layer (32) where the data received is propagated to one or more higher layers (33-37) of said network stack, said electronic device being connected to a communication network, in which method said network traffic is filtered and an unwanted data reception addressed to said electronic device filtered out, the method further comprising receiving (42) said network traffic in at least one said

Figure 4 shows a simplified flowchart for one or more methods according to another aspect of the invention. The figure shows:

1. Data for a frame, e.g. Ethernet frame, is received in the physical layer.
2. Data in part or whole of the frame is compared with the traffic rules for filtering;
3. If unwanted data is detected Y - then
4. Control signal asserted or control data appended (so that frame is subsequently discarded in the MAC)
5. If control signal is asserted or control data appended then data about that discarded frame may be logged;
6. If unwanted traffic not detected N then
7. The packet is propagated with original control signal(s) and original data to another network layer 33-37.

[0052] The electronic device may be installed and configured for use in a local node of a component connected to, and controlled by, a control system. Typically as a component controlled by a control system, a component such as a measuring instrument for example a sensor or transducer, or an actuator such as a valve, motor, pump, switch, or another component used in the control of industrial processes such as a pulp & paper process, metal forming process, or for controlling equipment such as transformers, breakers, isolators, switches and so on used eg in feeder installations, switch yards and substations for the generation, transmission or distribution of electrical power.

[0053] The functions of the filtering unit 3 or filtering circuit may be carried out by processing digital functions, algorithms and/or computer programs and/or by analogue components or analogue circuits or by a combination of both digital and analogue functions.

[0054] The methods of the invention may be carried out by means of one or more computer programs comprising computer program code or software portions running on a computer or a processor. The microprocessor (or processors) comprises a central processing unit CPU performing the steps of the method according to one or more facets of the invention. This is performed with the aid of one or more said computer programs, such as, which are stored at least in part in a memory storage device such as memory 6 and/or in control logic 8 and as such accessible by the one or more processors. The or each processor may be in a control unit, or part thereof.

It is to be understood that said computer programs may also be run on one or more general purpose industrial microprocessors or computers instead of one or more specially adapted computers or processors.

[0055] The computer program comprises computer program code elements or software code portions that make the computer perform methods such as that shown in the flowchart of Figure 4 using equations, algorithms, data, stored values and calculations previously described. A part of the program may be stored in a processor as above, but also in a ROM, RAM, PROM, EPROM or EEPROM chip or similar memory means. The program in part or in whole may also be stored on, or in, other suitable computer readable medium such as a magnetic disk, CD-ROM or DVD disk, hard disk, magnetic or optical memory storage means, in volatile memory, in flash memory, as firmware, stored on a data server or on one or more arrays of data servers. Other known and suitable media, including removable memory media such as memory sticks or other removable flash memories, hard drives etc. may also be used.

[0056] It should be noted that while the above describes exemplifying embodiments of the invention, there are several variations and modifications which may be made to the disclosed solution without departing from the scope of the present invention as defined in the appended claims.

Claims

1. A method of limiting the amount of network traffic reaching an electronic device operating an Ethernet networking protocol and using a network stack comprising at least one physical layer (31) communicating with at least one link layer (32) where the data received is propagated to one or more higher layers (33-37) of said network stack, said electronic device being connected to a communication network, in which method said network traffic is filtered and an unwanted data reception addressed to said electronic device filtered out, the method further comprising receiving (42) said network traffic in at least one said
2. The method according to claim 1, **characterised by** said filtering comprising inspecting said network traffic during reception and propagation from the at least one said physical layer (1) to at least one said link layer (32), and comparing (44) said network traffic with information from an access control list.

3. The method according to claim 1, **characterised by** detecting said unwanted data reception at the link layer (32) or media access controller (2) before it reaches another higher layer (33-37) of said network stack of said electronic device, **characterised in that** the filtering is arranged to append control data (46) to the reception such that the MAC of the link layer (2) rejects the said unwanted data reception transmitted from the physical layer (1).

4. The method according to claim 3, **characterised by** asserting a control line (9) such that the media access controller, MAC, detects a receiver error (RX_ERROR) and/or negated data valid (RX_DV) and/or other control line and discards the whole Ethernet frame containing said unwanted data reception.

5. The method according to claim 1, **characterised by** logging data (47) concerning discarded unwanted data packets and recording characteristics about the network traffic.

6. The method according to any previous claim, **characterised by** switching on filtering dependent on a number of data packets received per unit time, and then inspecting said network traffic during reception from the at least one said physical layer (PHY) to at least one said link layer (32) or media access controller, MAC.

7. The method according to any previous claim, **characterised by** switching on filtering dependent on an external signal and then inspecting said network traffic during reception from the at least one said physical layer (PHY) to at least one said link layer (32) or media access controller, MAC.

8. The method according to claim 1, **characterised by** switching on filtering dependent on the number of data packets received per unit time according to at least one predetermined number of data packets.

9. The method according to claim 1, **characterised by** inspecting said network traffic during reception from the at least one said physical layer (PHY) beginning inspection on receipt of a complete data packet.

10. The method according to any previous claim, **characterised by** inspecting said network traffic during reception from the at least one said physical layer (PHY) to at least one said link layer (32) or media access controller (2) by comparing with data in any from the group of: a list of accepted traffic, information based on an analysis of traffic, a list updated by a processor of said electronic device, a list of non-accepted traffic, an access control list.

11. An electronic device arranged for operation according to an Ethernet networking protocol using a network stack comprising at least one physical layer (PHY) (31) and communication to at least one link layer (32) or media access controller (2), wherein a filtering unit is arranged to filter said network traffic to said electronic device and filter out an unwanted data reception addressed to said electronic device, said filtering unit (3) being connected between said at least one physical layer (PHY) (1) and the link layer or media access controller, MAC (2), the filtering unit(3) being arranged with at least one switchable line or bus (11, 12) and control logic (8) for inspecting said network traffic during reception from the at least one said physical layer to at least one said link layer or media access controller, and for comparing said network traffic to at least one access control list and for detecting a said unwanted data reception, the filtering unit (3) being arranged for sending a signal (9) causing the selected said unwanted data reception to be rejected and discarded by the at least one said link layer (32) or media access controller (2) before it reaches another layer (33-37) of said network stack, the device being **characterised in that** the filtering unit (3) is arranged for appending control data upon detection of a said unwanted data reception such that the MAC of the link layer rejects the said unwanted data reception transmitted from the physical layer.

12. The device according to claim 11, **characterised in that** the filtering unit (3) is arranged for asserting a control line error by means of the switchable line or bus, upon detection of a said unwanted data reception.

13. The device according to claim 11, **characterised in that** the filtering unit (3) is arranged at least in part as a circuit realized in hardware.
14. The device according to claim 11, characterised in that the at least one said link layer (32) comprises a media access controller, MAC (2), which is arranged to reject the said unwanted data reception transmitted from the physical layer (PHY) so that it does not propagate to other layers (33-37).

15. The device according to claim 11, characterised in that it is connected to an external circuit from which it is arranged to receive information for determining in the control logic (8) a number of data packets received per unit time.

16. The device according to claim 11, characterised in that it comprises apparatus for logging data (47) concerning discarded unwanted data packets and/or recording characteristics about the network traffic.

17. A computer program for limiting the amount of network traffic reaching an electronic device operating an Ethernet networking protocol and comprising software code portions or computer code to cause a computer or processor to carry out all the steps of the method according to claim 1.

**Patentansprüche**

1. Verfahren zum Begrenzen der Menge von Netzwerkverkehr, die eine elektronische Vorrichtung erreicht, die ein Ethernet-Netzwerkprotokoll betreibt und einen Netzwerkstapel verwendet, der mindestens eine Bitübertragungsschicht (31) umfasst, die mit mindestens einer Verbindungsschicht (32) kommuniziert, wo die empfangenen Daten in eine oder mehrere höhere Schichten (33-37) des Netzwerkstapels weiterbewegt werden, wobei die elektronische Vorrichtung mit einem Kommunikationsnetzwerk verbunden wird, in welchem Verfahren der Netzwerkverkehr gefiltert und unerwünschter, an die elektronische Vorrichtung adressierter Datenempfang herausgefiltert wird, wobei das Verfahren ferner das Empfangen (42) des Netzwerkverkehrs in mindestens einer Bitübertragungsschicht (1) der elektronischen Vorrichtung, das Vergleichen des Netzwerkverkehrs mit mindestens einer Zugangssteuerungsliste, das Detektieren (45) des unerwünschten Datenempfangs und das Senden eines Signals, das veranlasst, dass der ausgewählte, unerwünschte Datenempfang in der Verbindungsschicht oder der Medienzugangssteuerung, MAC, (2) zurückgewiesen und verworfen wird, bevor er eine weitere, höhere Schicht (33-37) des Netzwerkstapels der elektronischen Vorrichtung erreicht, umfasst, dadurch gekennzeichnet, dass das Filtern ausgelegt ist zum Anhängen von Steuerdaten (46) an den Empfang, derart, dass die MAC der Verbindungsschicht (2) den unerwünschten Datenempfang, der von der Bitübertragungsschicht (1) übertragen wird, zurückweist.


5. Verfahren nach Anspruch 1, gekennzeichnet durch das Protokollieren von Daten (47) hinsichtlich verworferen, unerwünschter Datenpakete und das Aufzeichnen von Charakteristiken über den Netzwerkverkehr.

6. Verfahren nach einem der vorhergehenden Ansprüche, gekennzeichnet durch das Einschalten des Filters in Abhängigkeit von einer Anzahl von Datenpaketen, die pro Zeiteinheit empfangen wird, und dann Untersuchen des Netzwerkverkehrs, während des Empfangs von der mindestens einen Bitübertragungsschicht (PHY) zu mindestens einer Verbindungsschicht (32) oder der Medienzugangssteuerung, MAC.

7. Verfahren nach einem der vorhergehenden Ansprüche, gekennzeichnet durch das Einschalten des Filters in Abhängigkeit von einem externen Signal und dann Untersuchen des Netzwerkverkehrs, während des Empfangs von der mindestens einen Bitübertragungsschicht (PHY) zu mindestens einer Verbindungsschicht (32) oder der Medienzugangssteuerung, MAC.
8. Verfahren nach Anspruch 1, gekennzeichnet durch das Einschalten des Filters in Abhängigkeit von einer Anzahl von Datenpaketen, die pro Zeiteinheit empfangen werden, gemäß mindestens einer vorbestimmten Anzahl von Datenpaketen.

9. Verfahren nach Anspruch 1, gekennzeichnet durch das Untersuchen des Netzwerkverkehrs, während des Empfangens von der mindestens einen Bitübertragungsschicht (PHY), wobei die Untersuchung bei Empfang eines kompletten Datenpaketks begonnen wird.


11. Elektronische Vorrichtung, die ausgelegt ist zum Betrieb gemäß eines Ethernet-Netzwerkprotokolls unter Verwendung eines Netzwerkstapels, der mindestens eine Bitübertragungsschicht (PHY) (31) und Kommunikation mit mindestens einer Verbindungsschicht (32) oder Medienzugangsteuerung (2) umfasst, wobei eine Filtereinheit dafür ausgelegt ist, den Netzwerkverkehr zu der elektronischen Vorrichtung zu filtern und unerwünschten, an die elektronische Vorrichtung adressierten Datenempfang herauszufiltern, wobei die Filtereinheit (3) zwischen die mindestens eine Bitübertragungsschicht (PHY) (1) und die Verbindungsschicht oder Medienzugangssteuerung, MAC (2) geschaltet ist, die Filtereinstellung (3) mit mindestens einer schaltbaren Leitung oder einem Bus (11, 12) und einer Steuerlogik (8) zum Untersuchen des Netzwerkverkehrs, während des Empfangens von der mindestens einen Bitübertragungsschicht zu der mindestens einen Verbindungsschicht oder Medienzugangssteuerung, versehen ist, und zum Vergleichen des Netzwerkverkehrs mit mindestens einer Zugangssteuerungsliste und zum Detektieren des unerwünschten Datenempfangs, wobei die Filtereinstellung (3) ausgelegt ist zum Senden eines Signals (9), das veranlasst, dass der ausgewählte, unerwünschte Datenempfang von der mindestens einen Verbindungsschicht (32) oder Medienzugangssteuerung (2) zurückgewiesen und verworfen wird, bevor er eine weitere Schicht (33-37) des Netzwerkstapels erreicht, wobei die Vorrichtung dadurch gekennzeichnet ist, dass die Filtereinheit

(3) ausgelegt ist zum Anhängen von Steuerdaten bei Detektion des unerwünschten Datenempfangs, so dass die MAC der Verbindungsschicht den unerwünschten Datenempfang, der von der Bitübertragungsschicht übertragen wird, zurückweist.

12. Vorrichtung nach Anspruch 11, dadurch gekennzeichnet, dass die Filtereinheit (3) ausgelegt ist zum Ausüben eines Steuerleitungsfehlers mittels einer schaltbaren Leitung oder eines Busse, bei Detektion des unerwünschten Datenempfangs.

13. Vorrichtung nach Anspruch 11, dadurch gekennzeichnet, dass die Filtereinheit (3) zumindest teilweise als eine in Hardware realisierte Schaltung ausgelegt ist.

14. Vorrichtung nach Anspruch 11, dadurch gekennzeichnet, dass die mindestens eine Verbindungsschicht (32) eine Medienzugangsteuerung, MAC (2) umfasst, die dafür ausgelegt ist, den unerwünschten Datenempfang, der von der Bitübertragungsschicht (PHY) übertragen wird, zurückzuweisen, so dass er sich nicht in andere Schichten (33-37) weiterbewegt.

15. Vorrichtung nach Anspruch 11, dadurch gekennzeichnet, dass sie mit einer externen Schaltung verbunden ist, wobei die Vorrichtung dafür ausgelegt ist, von dieser Informationen zu empfangen zum Be- stimmen einer Anzahl von pro Zeiteinheit erhaltenen Datenpaketen in der Steuerlogik (8).


17. Computerprogramm zum Begrenzen der Menge von Netzwerkverkehr, die eine elektronische Vorrichtung erreicht, die ein Ethernet-Netzwerkprotokoll behandelt, und das Softwarecodeteile oder Computercode umfasst, um einen Computer oder Prozessor zu veranlassen, sämtliche Schritte des Verfahrens nach Anspruch 1 auszuführen.
Procédé selon l'une quelconque des revendications précédentes, caractérisé par l'activation d'un filtrage dépendant d'un nombre de paquets de données reçus par unité de temps, puis l'inspection dudit trafic réseau pendant la réception allant de l’au moins une couche physique (PHY) à au moins une dite couche de liaison (32) ou un dit contrôle d’accès au support, MAC.

7. Procédé selon l’une quelconque des revendications précédentes, caractérisé par l’activation d’un filtrage dépendant d’un signal externe puis l’inspection dudit trafic réseau pendant la réception allant de l’au moins une couche physique (PHY) à au moins une dite couche de liaison (32) ou un dit contrôle d’accès au support, MAC.

8. Procédé selon la revendication 1, caractérisé par l’activation d’un filtrage dépendant du nombre de paquets de données reçus par unité de temps selon au moins un nombre prédéterminé de paquets de données.

9. Procédé selon la revendication 1, caractérisé par l’inspection dudit trafic réseau pendant la réception venant de l’au moins une dite couche physique (PHY), l’inspection commençant à la réception d’un paquet de données complet.

10. Procédé selon l’une quelconque des revendications précédentes, caractérisé par l’inspection dudit trafic réseau pendant la réception allant de l’au moins une dite couche physique (PHY) à au moins une dite couche de liaison (32) ou un dit contrôle d’accès au support (2) par une comparaison à des données prises dans un quelconque des groupes parmi : une liste de trafic accepté, des informations basées sur une analyse de trafic, une liste mise à jour par un processeur dudit dispositif électronique, une liste de trafic non accepté, une liste de contrôle d’accès.

11. Dispositif électronique conçu pour fonctionner selon un protocole de réseau Ethernet utilisant une pile de réseau comprenant au moins une couche physique (PHY) (31) et pour communiquer vers au moins une couche de liaison (32) ou un contrôle d’accès au support (2), dans lequel une liste de filtrage est conçue pour filtrer dudit trafic réseau vers dudit dispositif électronique, une liste de trafic non accepté, une liste de contrôle d’accès.
un dit contrôle d'accès au support, et pour comparer ledit trafic réseau à au moins une liste de contrôle d'accès et pour détecter une dite réception de données indésirables, l'unité de filtrage (3) étant conçue pour envoyer un signal (9) faisant que ladite réception de données indésirables sélectionnée soit rejetée et éliminée par l'au moins une dite couche de liaison (32) ou un dit contrôle d'accès au support (2) avant qu'elle atteigne une autre couche supérieure (33-37) de ladite pile de réseau, le dispositif étant caractérisé en ce que l'unité de filtrage (3) est conçue pour joindre des données de commande lors de la détection d'une dite réception de données indésirables de manière à ce que le MAC de la couche de liaison rejette ladite réception de données indésirables transmise par la couche physique.

12. Dispositif selon la revendication 11, caractérisé en ce que l'unité de filtrage (3) est conçue pour activer une erreur de ligne de commande au moyen de la ligne ou du bus commutable lors de la détection d'une dite réception de données indésirables.

13. Dispositif selon la revendication 11, caractérisé en ce que l'unité de filtrage (3) est conçue au moins en partie comme un circuit réalisé sous forme matérielle.

14. Dispositif selon la revendication 11, caractérisé en ce que l'au moins une dite couche de liaison (32) comprend un contrôle d'accès au support, MAC (2), qui est conçu pour rejeter ladite réception de données indésirables transmise par la couche physique (PHY) pour qu'elle ne se propage pas à d'autres couches (33-37).

15. Dispositif selon la revendication 11, caractérisé en ce qu'il est connecté à un circuit externe à partir duquel il est conçu pour recevoir des informations afin de déterminer dans la logique de commande (8) un nombre de paquets de données reçus par unité de temps.

16. Dispositif selon la revendication 11, caractérisé en ce qu'il comporte un appareil servant à consigner des données (47) concernant des paquets de données indésirables éliminés et/ou à enregistrer des caractéristiques relatives au trafic réseau.

17. Logiciel servant à limiter la quantité de trafic réseau atteignant un dispositif électronique exploitant un protocole de réseau Ethernet et comprenant des parties de code logiciel ou de code informatique faisant qu’un ordinateur ou un processeur exécute toutes les étapes du procédé selon la revendication 1.
Fig. 2

Fig. 1
Standard Ethernet
Fig.3
OSI Model
Fig. 4

Start

42 Data for a Frame being received

44 Whole or part frame matched to filtering/traffic rule?

45 Y

46 Append control data or assert control signals

N

48 Propagate original control signals and control data

47 Log data about discarded frame
Fig. 5

- PHY with high speed serial lines
- Filtering circuit
- MAC

1' → 3' → 2'
REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader’s convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 6434118 B [0005]
- US 7280591 B [0005]
- US 2004073671 A [0006]